CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

Descifrador de contraseñas de John el Destripador

John the Ripper password cracker

Franklin Encalada [1]

[1,2] Universidad Tecnológica Israel–Carrera de Sistemas de Información, 170516, Quito, Ecuador

Fecha de recepción: marzo 2022 **Fecha de aprobación:** mayo 2022

RESUMEN

Con esta herramienta, los expertos en seguridad informática pueden ver si las contraseñas que definen son lo suficientemente seguras. El programa es muy flexible y permite ataques de diversas formas, incluidos ataques directos y ataques mediante sistemas de diccionario. Cuanto más esfuerzo pongas en descifrar códigos utilizando Jāni Uzškėrdėju, más confianza podrás tener en su eficacia. Implementar estas herramientas en su día a día puede brindarle una mayor confianza en la efectividad del sistema y la seguridad que brinda. Sin embargo, no son la única solución ideal ya que existen otras con propiedades similares que también pueden servir como buenos complementos. La cuestión de elegir entre uno u otro es ver cuál se adapta mejor a las vulnerabilidades que creemos que puede haber, o a las vulnerabilidades exactas que sufre nuestro entorno gestionado.

Palabras clave: hackear, the Ripper, plataformas.

ABSTRACT

With this tool, computer security experts can see if the passwords they define are secure enough. The program is very flexible and allows attacks of various forms, including direct attacks and attacks using dictionary systems. The more effort you put into deciphering codes using Jāni Uzškėrdėju, the more confidence you can have in its effectiveness. Implementing these tools in your day to day can give you greater confidence in the effectiveness of the system and the security it provides. However, they are not the only ideal solution as there are others with similar properties that can also serve as good supplements. The question of choosing between one or the other is to see which one best adapts to the vulnerabilities we think there may be, or to the exact vulnerabilities that our managed environment suffers.

Key Words: hack, the Ripper, platforms.

[1] Estudiante de Ingeniería en Sistemas, e1716478662@uisrael.edu.ec

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

1. INTRODUCCIÓN

John the Ripper usa un ataque por diccionario, un diccionario con palabras que pueden ser contraseñas típicas, y las va probando todas. Para cada palabra, la cifra y la compara con el hash a descifrar. Si coinciden, es que la palabra era la correcta.

Esto funciona bien porque la mayor parte de las contraseñas que usa la gente son palabras de diccionario. Pero John the Ripper también prueba con variaciones de estas palabras: les añade números, signos, mayúsculas y minúsculas, cambia letras, combina palabras, etc.

Además, ofrece el típico sistema de fuerza bruta en el que se prueban todas las combinaciones posibles, sean palabras o no. Éste es el sistema más lento, y usado sólo en casos concretos, dado que los sistemas anteriores (el ataque por diccionario) ya permiten descubrir muy rápidamente las contraseñas débiles.

A continuación, se menciona las características más relevantes:

- Optimizado para muchos modelos de procesadores.
- Funciona en muchas arquitecturas y sistemas operativos.
- Ataques de diccionario y por fuerza bruta.
- Muy personalizable (es software libre).
- Permite definir el rango de letras que se usará para construir las palabras y las longitudes.
- Permite parar el proceso y continuarlo más adelante.
- Permite incluir reglas en el diccionario para decir cómo han de hacerse las variaciones tipográficas.
- Se puede automatizar; por ejemplo, ponerlo en cron.

2. DESARROLLO

2.1 Plataformas disponibles

John the Ripper al principio fue diseñado para Unix, pero ahora funciona en al menos 15 sistemas operativos distintos: 11 tipos de Unix, MS-DOS, Windows, BeOS y OpenVMS. Se puede encontrar en la mayoría de distribuciones Linux.

Es software libre distribuido bajo la licencia GPL, aunque permite que algunas partes del programa se usen con otras licencias, y otras están bajo el dominio público. Si existe una nueva distribución esta no funcionará, pero vamos a la web indicada sin la última parte del enlace y vemos el archivo con el directorio completo y el nombre de la última versión.

Una vez descargado lo movemos al directorio **/usr/share** para evitar problemas con el comando **cp**

Figura 1.

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

El instituto de Ciber Seguridad español o INCIBE, publicó esta estadística de los ataques de fuerza bruta con los que los Hackers lograban atacar diferentes servidores y lograr sus objetivos. Como vemos los usuarios root y admin. son los más usuales en diferentes plataformas SSH de Internet. En el caso de servidores Windows, en lo que es usuario de administración de LDAP, sería Administrador y Administrator.

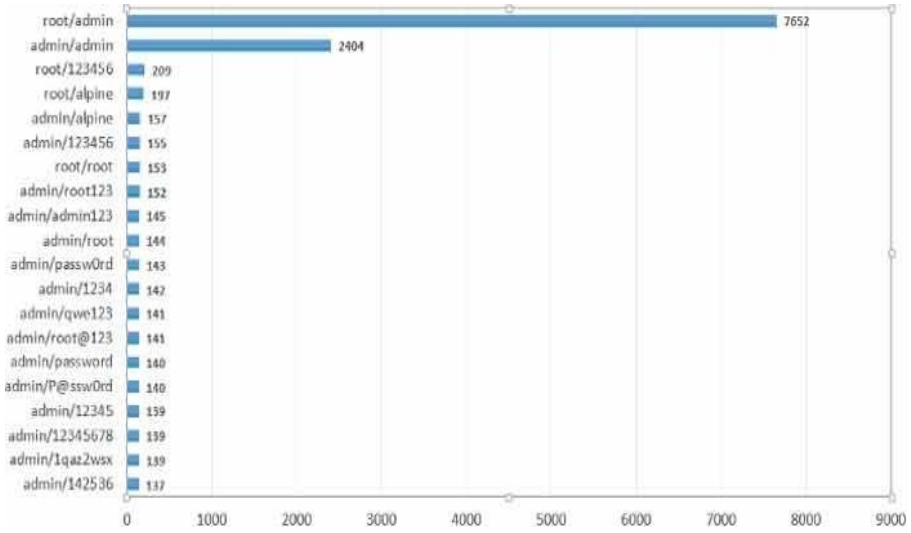

Figura 2.

Una de las aplicaciones más usadas por los **hackers** para atacar estas plataformas online es sin duda el John The Ripper, que sobre estos usuarios base, lanzan sus ataques de diccionario.

El ejemplo que vamos a realizar no será sobre un servidor externo para evitarnos problemas legales, vamos a atacarnos a nosotros mismos sólo para ver el funcionamiento correcto de esta aplicación.

Lo primero es descargarnos el programa, para ello ejecutamos **wget** (descarga) y la dirección con el programa.

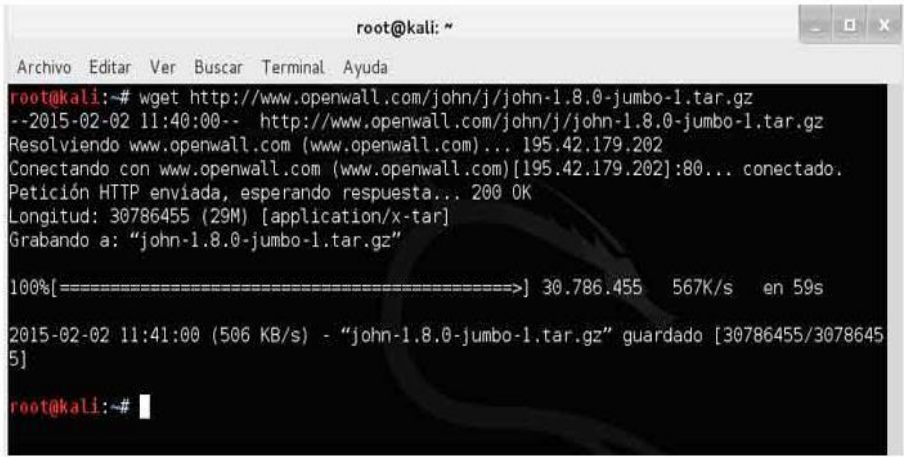

Figura 3.

En un sistema Unix, algunos usuarios malintencionados pueden intentar usar este programa para obtener información de acceso. Para evitarlo, basta con asegurarse de que las contraseñas cifradas no estén visibles en el fichero /etc/passwd, sino en el

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

fichero /etc/shadow, que *ha de tener desactivado el permiso de lectura* para los usuarios normales. Esta es la configuración predeterminada en los sistemas operativos de tipo Unix (BSD, GNU/Linux, Mac OS X, etc.)

Entramos en el directorio indicado y lo descomprimimos. Al estar en formato tar.gz, usamos **tar –xzvf**.

Figura 4.

Entramos en el directorio de la aplicación ya descomprimida **/John-1.8.0-jumbo-1/src/** con el comando **cd**.

Escribimos **make clean generic** y listo.

Figura 5.

Ejecutamos el John con el comando ./john –test.

Figura 6.

Copiamos el archivo de claves en el directorio de Jonh the ripper. El archivo /etc/shadow, es por defecto el archivo en el que Linux almacena las claves encriptadas.

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

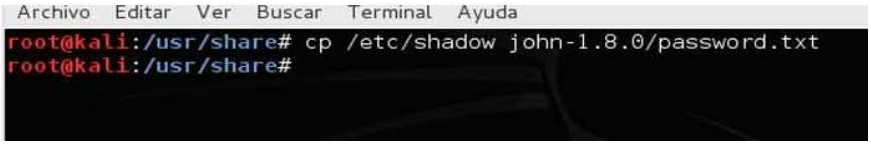

Figura 7.

Tardará un poco, pero saldrá algo así.

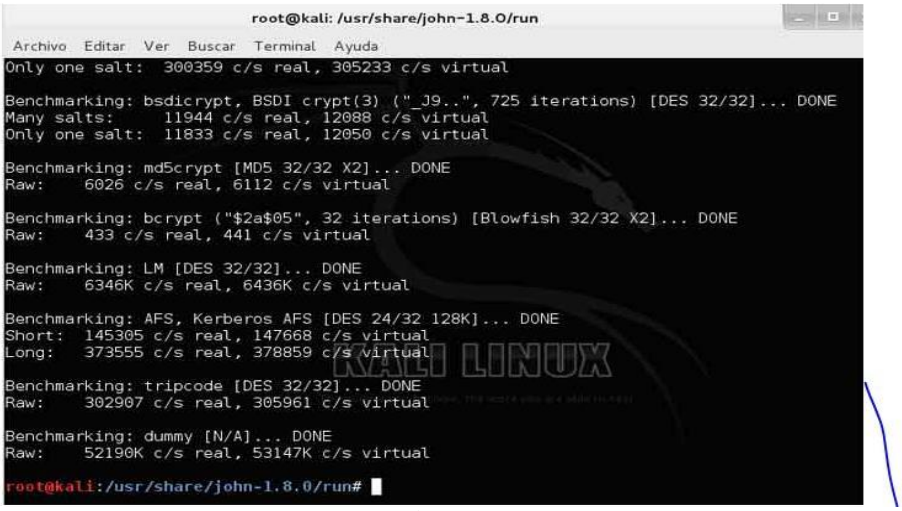

Figura 8.

Ahora vamos a usar el John The Ripper para buscar claves. Primero copiaremos el archivo **/etc/shadow** en el directorio **/root** desde otra terminal de comandos. Es el archivo sobre el que vamos a trabajar para extraer las contraseñas sin cometer delitos :)

Figura 9.

Ahora creamos usuarios con claves sencillas para ver su funcionamiento con el comando **adduser**.

Figura 10.

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

Entramos de nuevo en el directorio donde se ha instalado.

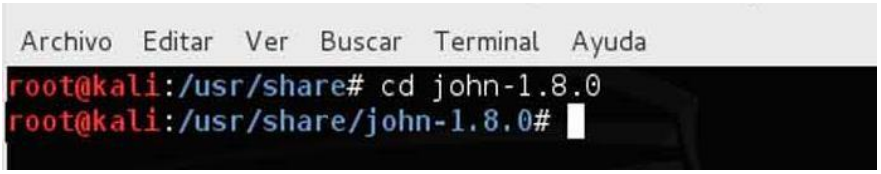

Figura 11.

Ejecutamos el comando **john –w=password.lst password.txt**, donde password.lst es el diccionario y password.txt el archivo de destino de las claves desencriptadas.

Figura 12.

Y ahora desencriptamos las contraseñas. Cuanto más sencillas sean más rápido irá, para ello ejecutamos **john –format=crypt password.txt**

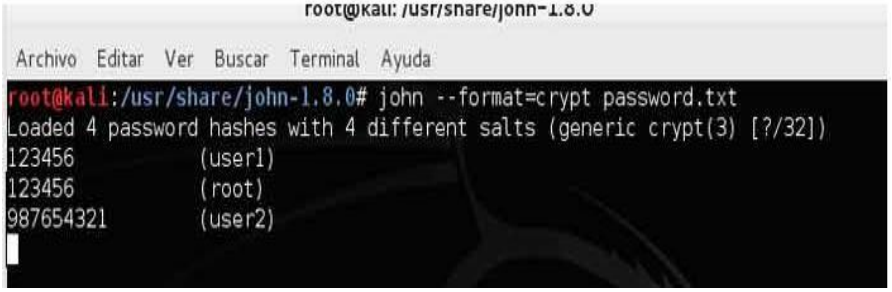

Figura 13.

2.2 Ataque Local de Contraseñas

Un ataque local de contraseñas depende en primera instancia de la habilidad para capturar los hashs desde un sistema objetivo. La manera de obtener estos datos es diversa, pero se requiere finalmente obtener los hashs de antemano

2.3 Función Hash Criptográfica

Una función hash criptográfica es una función hash considerada como prácticamente imposible de revertir, es decir recrear el dato de entrada desde únicamente el valor hash. La entrada se denimina algunas veces como mensaje, y el valor hash es denominada frecuentemente como resumen del mensaje o simplemente resumen.

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

2.4 Función Hash

Una función hash es cualquier función que puede ser utilizada para mapear datos de tamaño arbitrario hacia datos de tamaño fijo, con lo cual pequeños cambios en los datos de entradas producen cambios muy grandes en los datos de salida. Los valores de vuelto por una función hash son denominados como valores hash, códigos hash, sumas hash, o simplemente hashs.

Para la siguiente práctica se utilizará John The Ripper en Kali Linux, y la máquina virtual vulnerable Metasploitable2.

Se tiene acceso al sistema objetivo de evaluación con los permisos pertinentes para leer el archivo /etc/shadow.

cat /etc/shadow

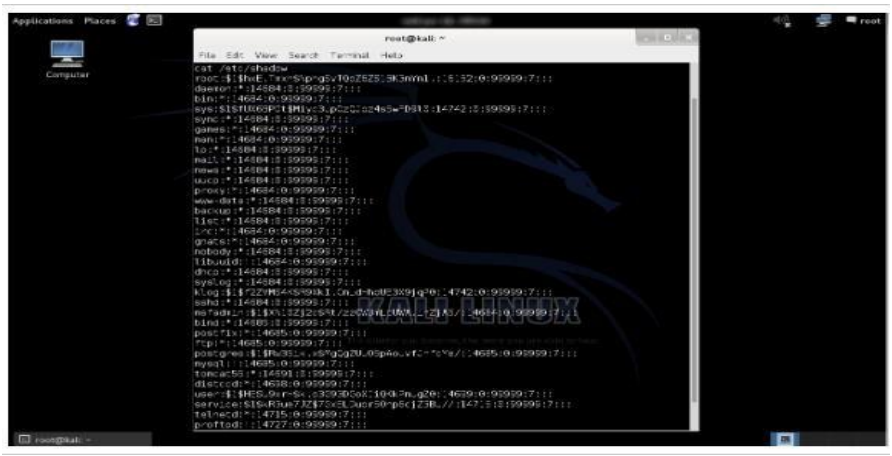

Figura 14.

Es de nuestro interés únicamente las cuentas de usuario que tienen asignada una contraseña. Se realiza para esto un sencillo filtrado usando el comando "grep".

grep '\$1\$' /etc/shadow

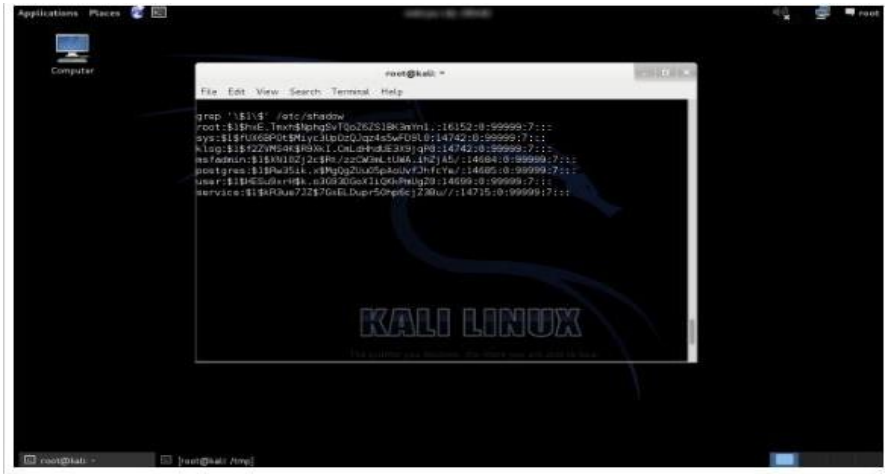

Figura 15.

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

La información de los hashes capturados se copiará a un archivo local en Kali Linux. Archivo contra el cual se ejecutará John The Ripper. El modo más simple para ejecutar John The Ripper es utilizando la opción "--single". El cual permite realizar un "cracking" sencillo.

Las reglas utilizadas en este modo serán leídas desde la sección [List.Rules:Single] del archivo de configuración de John The Ripper.

 # john --single hashes_m2

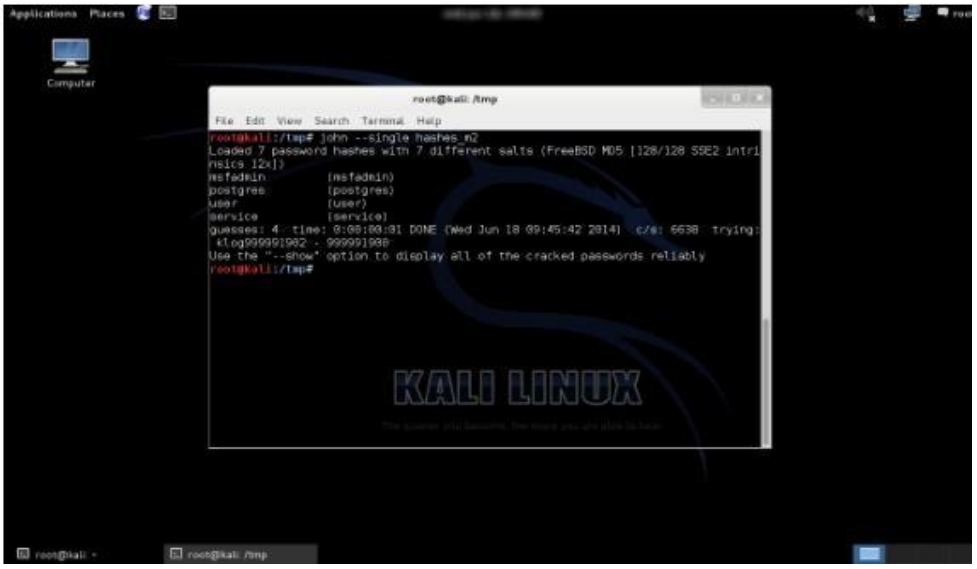

Figura 16.

El modo "wordlist" o lista de palabras definida con la opción "--wordlist=", permite la utilización de una lista de palabras.

 # john --wordlist=/usr/share/wordlists/diccionario.txt hashes_m2

Figura 17.

Con este último procedimiento realizado se han obtenido todas las contraseñas contenidas en el archivo. Se procede a visualizar está información utilizando la opción "--show".

 # john --show hashes_m2

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

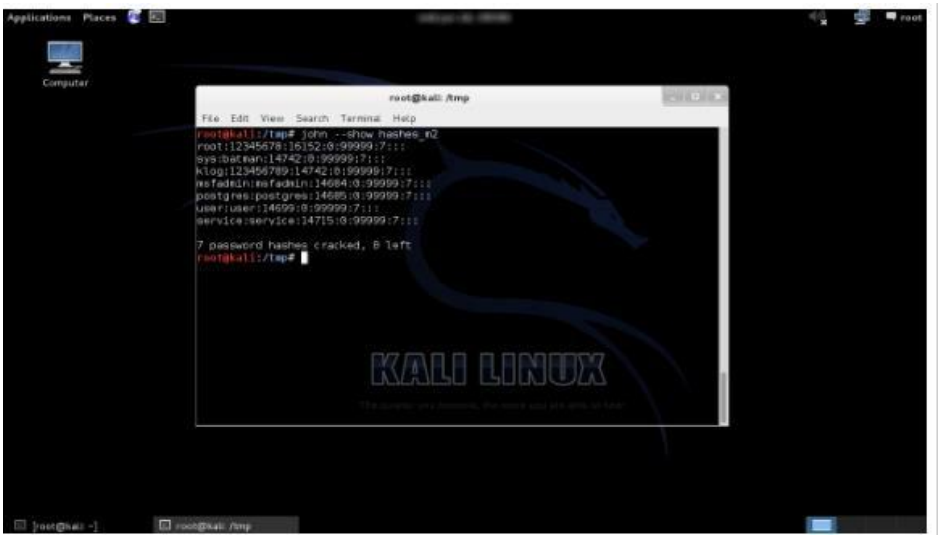

Figura 18.

Para las siguientes prácticas se utilizará los hashes de otro archivo "/etc/shadow" capturado desde otro sistema, al cual se le asigna el nombre "shadow1".

Además de la opción "--wordlist=" se utiliza la opción "--rules", la cual habilita las reglas de manipulación para la lista de palabras definida en el modo "wordlist". Estas reglas son leídas de [List.Rules:Wordlist].

 # john --wordlist=/usr/share/wordlists/diccionario.txt --rules shadow1

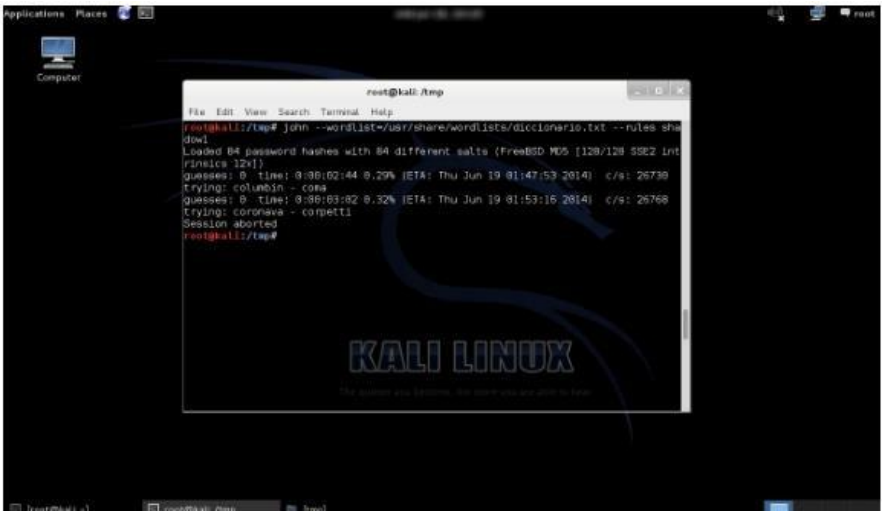

Figura 19.

John The Ripper permite también utilizar el modo "Incremental" o Incremental, que es un símil a realizar un ataque por fuerza bruta usando todas las combinaciones posibles de un conjunto de caracteres para la construcción de posibles contraseñas. En la siguiente práctica se utiliza "alpha" para utilizar todas las letras del alfabeto. Este información se define en la sección [Incremental:MODE] del archivo de configuración.

 # john --incremental:alpha shadow1

CREANDO INGENIOS
ISSN: 3028-8924
Correo: editor.revista@tecnologicoismac.edu.ec
URL: https://ismaconline.net/investigacion/index.php/CreaIngenio_2021/index
Volumen 2, Número 1 / Enero – Junio 2022 pp. 49-59

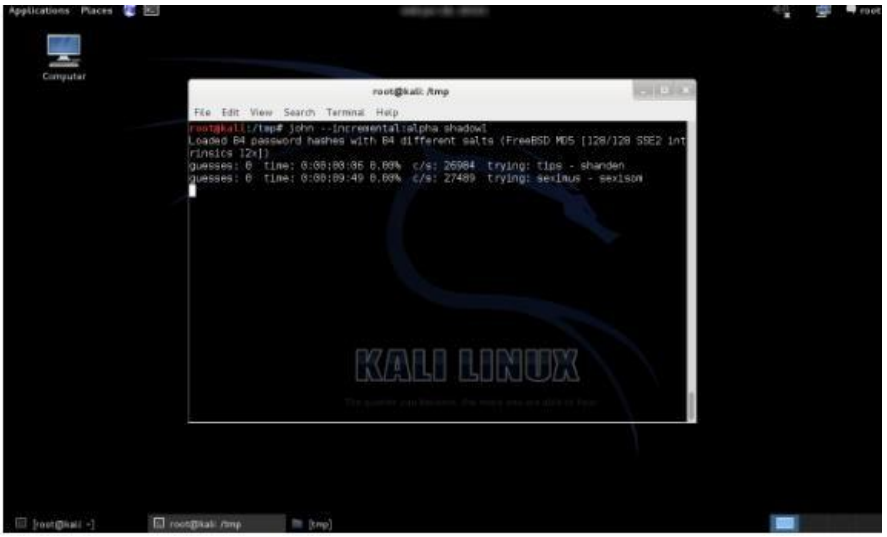

Figura 20.

John The Ripper tiene también un modo "External" o Externo utilizando las funciones definidas en la sección [List.External:MODE].

Uno de los puntos resaltantes e importantes en el procedimiento de realizar ataques locales de contraseñas, es el hecho de utilizar buenos diccionarios o listas de palabras a medida para maximizar las probabilidades de obtener resultados satisfactorios.

2.5 Instalación

John puede instalarse desde los repositorios de Debian/Ubuntu con un simple comando APT-GET, sin embargo en muchas ocasiones no viene con la última versión disponible, por lo tanto se recomienda descargar el código fuente desde el sitio oficial (http://www.openwall.com/) y proceder con la instalación manual que consta de los siguientes pasos:

1. Descarga la última versión de John y descomprimir el fichero tar.gz en un directorio.
2. Navegar hasta el directorio src/ donde se encuentran los ficheros fuente y ejecutar uno de los dos siguientes comandos:
   - make clean generic: Para ejecutar una instalación genérica.
   - make clean <SISTEMA>: Para ejecutar una instalación específica para un sistema determinado, esta opción es útil cuando se quiere distribuir el programa en una plataforma especifica (como por ejemplo DOS de windows):
   - make clean dos-djgpp-x86-any
   - make clean win32-cygwin-x86-any
   - make clean linux-x86-64

Los posibles valores pueden ser consultados con ejecutar simplemente el comando *make* sin ningún parámetro, de esta forma john listará los posibles valores que admitirá el campo <SISTEMA> Esta opción es recomendable en instalaciones que se mueven a una maquina distinta, por cuestiones de rendimiento, ya que cuando se ejecuta con la opción *generic* en tiempo de compilación se instancian características que mejoran el rendimiento de john en el sistema donde se está creando la instalación, sin embargo, si esta misma instalación se mueve a un sistema operativo con una arquitectura distinta el resultado puede ser distinto al esperado.

1. Una vez ejecutado el comando make correspondiente a la plataforma (o generic) navegar hasta el directorio run/ desde allí ejecutar el comando: *./john –test*

3. CONCLUSIONES

Este programa está perfeccionado para muchos modelos de procesadores, tiene un diccionario con palabras, que pueden ser contraseñas típicas, permite descubrir muy rápidamente las contraseñas débiles, y se ejecuta desde una línea de comandos.

Puede instalarse desde los repositorios de Debian/Ubuntu con un simpe comando APT-GET. Permite establecer de qué manera se va a realizar el interno de obtención de las credenciales encriptadas. Además, le permite a un programador incluir rutinas escritas en un subconjunto de lenguaje.

Por otro lado, es compatible con todos los modos simplemente utilizando la opción make-charset, es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros, adicionalmente, tiene la capacidad de descifrar claves complejas por lo tanto debemos de cambiar nuestra contraseña periódicamente.

REFERENCIAS

1. https://es.wikipedia.org/wiki/John_the_Ripper
2. http://www.cursodehackers.com/JohnTheRipper.html.
3. https://thehackerway.com/2011/05/19/conceptos-basicos-sobre-tecnicas-de-crackeo-con-john-the-ripper/
4. http://www.reydes.com/d/?q=Ataque_Local_de_Contrasenas_utilizando_John_The_Ripper
5. https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
6. https://www.redeszone.net/seguridad-informatica/john-the-ripper-crackear-contrasenas/
7. https://www.skamasle.com/crakear-con-john-the-ripper/